(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 065 861 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.01.2001 Bulletin 2001/01

(51) Int Cl.[7]: **H04L 29/06**, H04L 9/32, G06F 1/00

(21) Application number: **99401613.7**

(22) Date of filing: **28.06.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

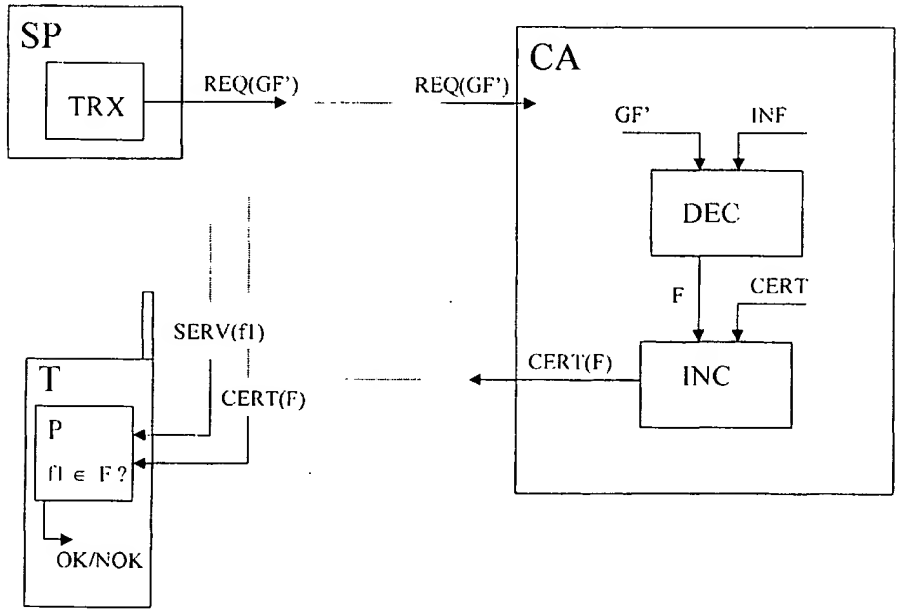
(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventor: **Penders, Alain**
3590 Diepenbeek (BE)

(74) Representative: **Narmon, Gisèle Marie Thérèse**
Alcatel Bell N.V.
Francis Wellesplein 1
2018 Antwerpen (BE)

(54) Method to provide authorization, a certifying authority, a terminal, a service provider and a certificate realizing such a method

(57) The invention relates to a method for use in a telecommunication environment. The method provides authorization by a certifying authority (CA) to a service provider (SP) whereby the service provider (SP) is allowed to execute predefined functionality (F) when a service is provided by the service provider (SP) to a terminal (T) of a user. The method includes the step of delivering a certificate (CERT) by the certifying authority (CA) to the service provider (SP). Moreover the method comprises the step defining in the certificate (CERT) a definition of the predefined allowed functionality (F) that is part of a global functionality (GF) supported in the telecommunication environment. Furthermore the invention concerns a certifying authority (CA), a service provider (SP) and a terminal (T) to realize the method.



Figure

EP 1 065 861 A1

Description

[0001] The present invention relates to a method to provide authorization as described in the preamble of claim 1, to a certifying authority, a terminal, a service provider and a certificate realizing such a method as described in the preamble of claim 7, claim 8, claim 9 and claim 10 respectively and to a telecommunication network comprising such a certifying authority, such a terminal and such a service provider as described in the preamble of claim 11.

[0002] Such a method for use in a telecommunication environment to provide authorization by a certifying authority to a service provider to execute predefined functionality in the event when a service is provided by the service provider to a terminal of a user, is already known in the art. Indeed, in such an event the certifying authority delivers a certificate to the service provider that provides the service provider the authorization to execute all the functionality of the telecommunication environment. Such a certificate is explained in the *'Frequently asked questions about today's cryptography, version 4.0' published by RSA laboratories, a division* of *RSA* Data *Security in* 1998. *Herein, the answer to question 4.1.3.10.* 'What are certificates' describes the object of a certificate. Certificates are digital documents attesting to the binding of a public key to an individual or other entity. They allow verification of the claim that a specific key does in fact belong to a specific individual. Certificates help to prevent someone from using a phony key to impersonate someone else. Certificates are typically used to generate confidence in the legitimacy of a public key. In some cases it may be necessary to create a chain of certificates, each one certifying the previous one until the parties involved are confident in the identity in question. Such a certificate contains a public key and name. As commonly used, a certificate also contains an expiration date, the name of the certifying authority that issued the certificate and a serial number. Most importantly, it contains the digital signature of the certificate issuer. The most widely accepted format for certificates is defined by the *ITU-T X.509 international standard.* Thus certificates can be read or written by any application complying with X.509.

[0003] Another application of certificates is described in the *WAP WTLS,* Version *30-Apr-1998, Wireless Application Protocol, Wireless Transport Layer Security specification.* Herein the content of such a certificate is described at page 57, paragraph 10.5.2 : a version of the certificate, the algorithm used to sign the certificate, the certification authority who signed the certificate, the validity period of the certificate, the owner of the key, the type of the key, parameters relevant for the public key and the public key that is being certified. The use of such certificates is described now in the following paragraph.

[0004] A service provider can send a service to a terminal of a user. These services can contain functions that do e.g. call control on the phone whereby any service provider can take over control of the phone e.g. make calls and accept or reject calls. In order to prevent malicious service providers from abusing someone's phone, a certificate based authentication system is used. Only if the service provider can present a certificate that is signed by a certifying authority e.g. a telecommunication network operator, the service provider is allowed access to these dangerous functions. The service provider is allowed to use predefined functionality when the service is provided by the service provider to a terminal of the user.

[0005] It has to be remarked that the expression 'a service is provided by the service provider' means that for instance the content of a service is executed by a terminal of the user. When such predefined function is to be executed by the terminal, first, the terminal controls the presence of a signed certificate for the service provider. When such certificate is available the function might be executed without e.g. any danger for abuse of the terminal.

[0006] A further remark is that a certifying authority can be a network operator itself. However, according to actual trends, such certifying authority can be a service provider itself that provides the service to a network operator of the management of giving or refusing such certificates.

[0007] Yet, it has to be remarked that the verification of the existence of a signed certificate implies different steps like a certification process, a certificate distribution and validation whereby public key / private key PKI algorithms are involved in order to provide a digital signing of the certificate. These steps are known steps to a person skilled in the art and are therefor not described in details here. The aim is the signing of a certificate and the fact that this signature can be controlled.

[0008] A problem outstanding with the existing certificates is that they are all or nothing solutions. This means that a service provider can get access to all functions or to no function i.e. a certificate is delivered or no certificate is delivered by the certifying authority.

[0009] Such a situation is often not sufficient for a network operator. Indeed, a network operator can not risk that a service provider may eventual by accident disable services to some terminals.

[0010] The problem becomes more clear with the following example. Presume a situation where a network operator trusts some service provider enough to let him modify the digital personal telephone book of a user, but the network operator does not trust the service provider enough to give him access to all functionality i.e. delivering a certificate. A solution to this problem is to add this function to the public library. This means that the network operator allows the use of this function by all service providers according to predefined specifications e.g. specifying the function in such a way that the user is previously asked permission by a service provider to add a predefined entry in its telephone book. However, in such an event, also service providers that are trusted

completely should work with the public function. Otherwise, both functions must be created i.e. one public function and one non-public function. This is resulting in a very complex, resource expensive and still not completely satisfying specification.

[0011] The object of the invention is to provide a method to provide authorization by a certifying authority to a service provider to execute predefined functionality, such as the above known methods, but which does not have the above mentioned drawbacks of dividing service providers into trusted or not trusted service providers.

[0012] The invention solves the problem by dividing the service providers into more detailed categories by giving a service provider access only to well specified functionality. This is realized by comprising in the certificate of a service provider a definition of the predefined functionality which is allowed to be executed by the service provider and which is part of the global functionality that supports the telecommunication environment. This is described by the method of claim 1 and is realized by the certifying authority of claim 7, the terminal of claim 8, the service provider of claim 9 and the certificate of claim 10 that are included in the telecommunication network of claim 11.

[0013] Indeed, by storing detailed information inside the certificate that is signed by the certifying authority, fine grained access control by the operator is possible. This drastically reduces the risk for an operator. In this way, a service provider can be allowed to use e.g. a predefined telephone function on a terminal without being able to damage the terminal or the network.

[0014] It has to be remarked that according to the prior art solutions a terminal controls first the presence of a signed certificate before its executes an included function of a service provided by a service provider. According to the present invention, the terminal controls not only the presence of a signed contract but also the presence of the definition of a predefined function in the signed contract before it executes the function in the event when a service is provided that includes this function.

[0015] A drawback of the present invention is however that the certificate gets larger by comprising a definition of the allowed functionality. A characteristic feature that is a solution to this drawback is described in claim 2. Indeed, by introducing an hierarchical tree-like structure in the organization of the global functionality the definition of the predefined allowed functionality can at least partly be realized by a definition of a branch of the structure. Hereby authorization is provided to predefined functions of the predefined functionality that are related to the branch. In this way also libraries identifiers and function identifiers as defined by the wireless mark-up script language can be used to be mentioned in order to provide authorization for, either one function, all functions from one library or all functions in all libraries : e. g. enable-all, enable-library-identifier, enable-function-identifier.

[0016] A further improvement of the definition of the predefined allowed functionality in the certificate is realized with claim 3. Herein it is described that the definition of the predefined functionality is at least partly realized by a revocation of part of the global functionality. This is e.g. implemented by using not only an 'enable' function with an allowed function as argument but also by using an 'disable' function with a revoked function as argument. Herewith, authorization to all functions of a library except one can easily be realized by enabling the library and disabling the revoked function.

[0017] A further implementation is described in claim 4. Herein it is described that the definition of the predefined functionality comprises definitions of wireless mark-up script language. Indeed, such implementation takes the advantage of making use of already existing and defined functions in a common known scripting language. These functions are described in a *specification: 'Wireless Application Protocol Wireless Markup Language Script WMLScript Language Specifications, version 30 April 1998 published by the WAP Wireless Application Protocol Forum.*

[0018] Another example of existing script language functions is provided e.g. by the Javascript language functions.

[0019] Furthermore, as already mentioned above, the Wireless Telephony Application Interface libraries are organizing wireless mark-up script language functions into predefined functions and libraries such as call control, sending of short messages or managing a phone book. These functions and libraries of the wireless telephony application functions can also be used to define the allowed predefined functionality in the certificate. They are specified in the *'Wireless Application Protocol Wireless Telephony Application Interface specifications, from the WAP forum and published at April 30, 1998.* This is described in claim 5.

[0020] Yet the definitions of standard functions of a terminal are introduced into the definition of the allowed predefined functionality. Indeed, by introducing standard functions as specified according to the *'Wireless Application Protocol WMLScript Standard Libraries Specifications, published by the WAP Forum at april 30, 1998'* a service provider is allowed to use this standard functionality in order to provide e.g. calculator application. This is described in claim 6.

[0021] Finally it has to be remarked that the above mentioned WTAI functions as defined above are known to a person skilled in the art. These functions are valid for common known mobile terminals. However, additional functions can be defined in addition to the WTAI specifications according to the type of network used. An example is provided for a GSM addendum, an IS-136 (TDMA Time Division Multiple Access Cellular PCS Personal Communication System Radio Interface - Mobile Station - Base Station - compatibility) addendum and a PDC Pacific Digital Cellular addendum for WTAI, which

are specified, respectively, in :

- Wireless *Application Protocol Wireless Telephony application Interface specification, GSM Global system for Mobile Telecommunication specific Addendum, published by the WAP forum at April 30, 1998; and*
- *Wireless Application Protocol Wireless Telephony application Interface specification, IS-136 specific Addendum, published by the WAP forum at April 30, 1998; and*
- *Wireless application Protocol wireless Telephony application Interface Specification, PDC specific Addendum, published by the WAP forum, April 30, 1998.*

[0022] It should be noticed that the term 'comprising", used in the claim, should not be interpreted as being limitative to the means listed thereafter. Thus, the scope of the expression "a device comprising means A and B" should not be limited to devices consisting only of components A and B. It means that with respect to the present invention, the only relevant components of the device are A and B.

[0023] Similarly, it is to be noted that the term "coupled", also used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression "a device A coupled to a device B" should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that their exists a path between an output A and an input B which may be a path including other devices or means.

[0024] The above and other objects and features of the invention will become more apparent and the invention itself will be best understood by referring to the following description of an embodiment taken in conjunction with the accompanying figure which illustrates a telecommunication network.

[0025] First, the working of the method of the present invention will be explained by means of a functional description of the functional blocks shown in the figure. Based on this description, implementation of the functional blocks will be obvious to a person skilled in the art and will therefor not be described in further detail. In addition, the principle working of the method to provide authorization will be described.

[0026] Referring to the figure a telecommunication environment is shown. The telecommunication environment comprises a certifying authority CA, a terminal T of a user and a service provider SP.

[0027] The certifying authority CA is coupled via a telecommunication network to the service provider SP and to the terminal T. Also the service provider SP and the terminal T are coupled to each other via the telecommunication network. However, in order not to overload the Figure, this telecommunication network is in the Figure only shown in a simple way of inputs and outputs of the different included elements. Furthermore it has to be understood that it is clear to a person skilled in the art that such a telecommunication network includes more than one service provider SP, more than one terminal T and even might include more than one certifying authority. Since the invention can be explained only by mentioning the different above elements more elements are not shown in the figure.

[0028] The certifying authority CA comprises a decider DEC and an including means INC coupled thereto. The decider DEC is coupled between an input of the certifying authority CA and the including means INC. The including means INC is on its turn coupled to an output of the certifying authority CA.

[0029] The decider DEC is included to decide whether the service provider SP is entitled to execute at least part of the global functionality GF' of the telecommunication environment. In order to make this decision the decider DEC makes use of predefined information. This information can be implemented by means of a memory e.g. a database that keeps track of the different service providers and its allowed functionality. On the other hand an operator of the certifying authority CA might give an input in order to provide the predefined information only in the event when the question arises. The decider DEC is enabled to make decisions regarding the global functionality of the telecommunication environment according to predefined rules and conditions. This means that eventual e.g. for part of the global functionality GF the question never arises since the involved network operator prefers to keep this part only for its own purposes. On the other hand, the decider DEC is able to take requests of the service providers into account. In this way the decider DEC is enabled to make only a decision for the requested functionality by a service provider SP and saves hereby processing time. The decider DEC provides a result of its decision that is the allowed functionality F. The allowed functionality is provided by the decider DEC to the including means INC.

[0030] The including means INC comprises the allowed functionality F into the certificate CERT. According to this preferred embodiment this is realized with three predetermined functions: enable, disable and all. The inclusion means INC uses these predetermined functions upon the list of global functionality GF. The global functionality GF is organized in an hierarchical tree-like structure. The structure comprises libraries i.e. the branches of the tree and functions i.e. the ends of the branches. The libraries and the functions are used as the arguments of the predetermined functions. In this way, the including means INC is enabled to comprise the result of the decider DEC in a clear and concise way into the certificate CERT. The certificate is transmitted to the service provider SP but is also transmitted to other locations into the network. Indeed, it has to be explained that, as it is known to a person skilled in the art, these certificates might be consulted on predefined public locations in the telecommunication environment.

[0031] The service provider SP comprises a transmitter TRX. The transmitter is coupled to an output of the service provider SP. The transmitter TRX is included to transmit a request REQ(GF') of the service provider SP that includes a definition of the functionality where for the service provider SP desires access.

[0032] This request REQ(GF') is transmitted to the certifying authority CA. As it is known to a person skilled in the art, a service provider SP also receives a response of the certifying authority CA. In the event when the service provider SP is allowed to receive a certificate CERT, the certificate includes according to the present invention a definition of the allowed functionality F.

[0033] The terminal T comprises a processor P. The processor is included to verify the presence and the content of a certificate. Indeed, in the event when a user desires to use a service SERV of the service provider SP and this service comprises the execution of a predefined function f1, the certificate CERT will first be checked upon the authorization of this execution. Therefor the certificate CERT is extracted from the predefined location in the network. This checking might be performed at the moment when the service SERV is being provided but might be as well executed in advance. Indeed, it is possible that the user used this service SERV some time ago and that the certificate was already checked by that time. In this way, the result might still be stored in a cache of the terminal T. On the other hand, it might as well be the content of the certificate that is still stored in a cache of the terminal T whereby the certificate CERT(F) does not need to be extracted from a predefined location in the network anymore.

[0034] The processor P provides hereby a result OK/NOK that authorizes or revokes, respectively, the access to the function f1 whilst the service SERV is executed.

[0035] The following paragraph describes the principle working of the present invention.

[0036] Presume a situation wherein the service provider SP wants to provide a service SERV that comprises the function f1 call set-up. The service provider SP never provided such a service SERV that includes this functionality, so the service provider SP first has to get to permission to access the call set-up function of a terminal T. The service provider SP transmits a request REQ with its transmitter TRX to the certifying authority CA. For this particular embodiment it is preferred to work with a certifying authority CA that only takes into account the requested functions. In this way the certifying authority saves processing time. Thus, the service provider SP comprises in its request the required functionality GF' i.e. the call set-up function f1. The certifying authority CA receives the request from the service provider SP and decides by means of its decider DEC whether the authorization is allowed. The decider DEC takes here for predefined information INF into account. According to this predefined information INF the service provider SP is a trustable service provider and is allowed by the decider DEC to execute the call set-up function when providing a service SERV to a user. The decider provides this result to the including means INC. The including means INC comprises this result into a prepared certificate CERT for the service provider SERV. The including means INC uses the enable predetermined function in order to provide authorization to the functionality related to the call set-up function f1. The definition becomes: enable-library(WTAI.WTAcall--handling). The certificate is provided by the certifying authority CA to the service provider SP and is also distributed into the network towards a predefined location.

[0037] In the event when a user desires to make use of the service SERV of the service provider SP, at a certain moment during execution of the different steps of the service SERV the terminal T will be requested to execute the function f1 call set-up function. In stead of executing this functionality immediately the terminal T will request for the existence of a certificate CERT(F) from the service provider SP. Since the terminal can find the certificate CERT at the predefined location into the network, the terminal T will download the certificate CERT. Whilst the certificate CERT is controlled upon its signature it will also be checked by the processor P of the terminal T upon the definitions of the allowed functionality F. Since the certificate CERT of the service provider indeed comprises the definition of the call set-up functionality F, the execution of the function f1 call set-up is allowed. This result is stored in a cache of the terminal T and the terminal T proceeds the execution of the desired service SERV by executing the call-set up function f1.

[0038] While the principles of the invention have been described above in connection with specific apparatus, it is to be clearly understood that this description is made only by way of example and not as a limitation on the scope of the invention, as defined in the appended claims.

Claims

1. A method for use in a telecommunication environment to provide authorization by a certifying authority (CA) to a service provider (SP) to execute predefined functionality (F) when a service is provided by said service provider (SP) to a terminal (T) of a user, said method includes the step of delivering a certificate (CERT), **characterized** in that said method further comprises the step of comprising in said certificate (CERT) a definition of said predefined functionality (F), said predefined functionality (F) being part of a global functionality (GF) supported in said telecommunication environment.

2. The method according to claim 1, characterized in that said global functionality (GF) is organized according to a hierarchical tree-like structure and that

said definition of said predefined functionality (F) is at least partly realized by a definition of a branch of said structure whereby authorization is provided to predefined functions of said predefined functionality (F) that are related to said branch.

3. The method according to anyone of the previous claims, characterized in that said definition of said predefined functionality (F) being at least partly realized by a revocation of part of said global functionality (GF).

4. The method according to anyone of the previous claims, characterized in that said definition of said predefined functionality (F) comprises definitions of wireless markup script language.

5. The method according to anyone of the previous claims, characterized in that said definition of said predefined functionality (F) comprises definitions of wireless application protocol wireless telephony application functions.

6. The method according to anyone of the previous claims, characterized in that said definition of said predefined functionality (F) comprises definitions of wireless application protocol wireless markup language script standard functions.

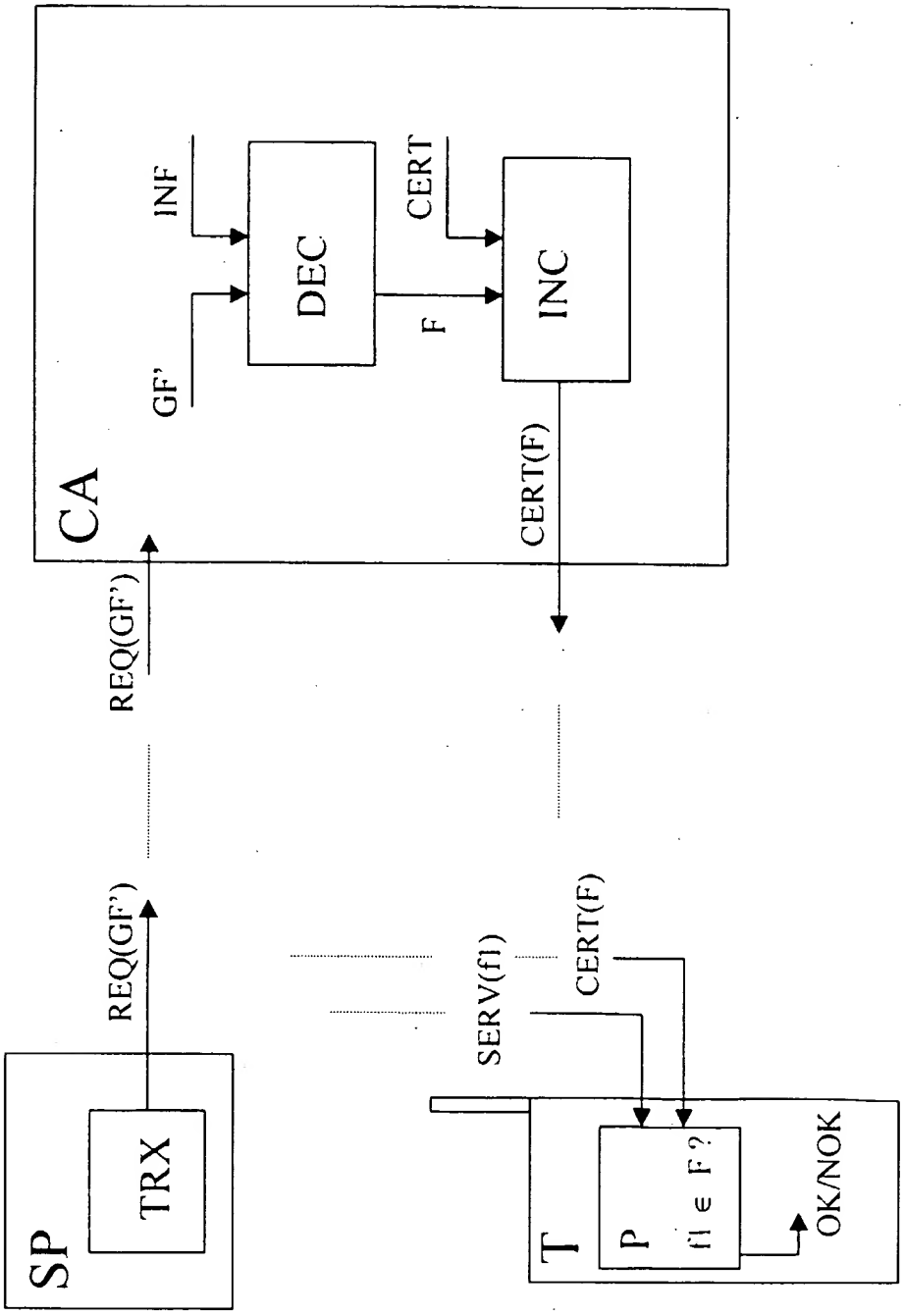
7. A certifying authority (CA) to realize the method according to any one of claim 1 to claim 6, characterized in that said certifying authority (CA) comprises decision means (DEC) to decide according to predefined information (INF) whether said service provider (SP) is entitled to execute at least part of said global functionality (GF') and to provide thereby an allowed functionality (F), and inclusion means (INC) coupled thereto to include in said certificate (CERT) a definition of said allowed functionality (F), said allowed functionality (F) being constituted by said predefined functionality (F).

8. A terminal (T) to realize the method according to any one of claim 1 to claim 6 characterized in that said terminal (T) comprises processing means (P) to check said certificate (CERT) upon a presence of a definition of a function (f1) of said global functionality (GB) before execution of said function (f1) and to provide thereby any one of authorization and revocation of the execution of said function (f1) by said service provider (SP) in the event when said service (SERV) is provided by said service provider (SP) to said terminal (T).

9. A service provider (SP) to realize the method according to any one of claim 1 to claim 6, characterized in that said service provider (SP) comprises transmitting means (TRX) to forward a request (REQ) to said certifying authority (CA) in order to receive said authorization, said request (REQ) comprises a definition of at least part of said global functionality (GF').

10. A certificate (CERT) to realize the method according to any one of claim 1 to claim 6, characterized in that said certificate (CERT) comprises a definition of said predefined functionality (F) being part of a global functionality (GF) supported in said telecommunication environment.

11. A telecommunication network characterized in that said telecommunication network comprises any one of a certifying authority (CA), a terminal (T) and a service provider (SP) according to claim 7, claim 8 and claim 9, respectively.


CA
INF
GF'
DEC
CERT
F
INC
CERT(F)
REQ(GF')
REQ(GF')
SP
TRX
SERV(f1)
CERT(F)
T
P
f1 ∈ F ?
OK/NOK

Figure

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 40 1613

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	TAYLOR A: "OVER-THE-AIR SERVICE PROVISIONING" ANNUAL REVIEW OF COMMUNICATIONS, XP000793196 * page 953, left-hand column, line 1 - page 956, left-hand column, line 6 *	1,7-11	H04L29/06 H04L9/32 G06F1/00
A	US 5 412 717 A (FISCHER ADDISON M) 2 May 1995 (1995-05-02) * abstract * * column 2, line 24 - column 3, line 10 * * column 5, line 3 - column 6, line 24 * * column 8, line 45 - column 9, line 18 * * figures 2,3 *	1,7-11	
A	WO 96 02993 A (BANKERS TRUST CO ;SUDIA FRANK W (US); SIRITZKY BRIAN (US)) 1 February 1996 (1996-02-01) * page 11, line 23 - page 12, line 1 * * page 15, line 9 - page 21, line 1 * * page 27, line 25 - page 28, line 4 *	1,7-11	
A	MARIE ROSE LOW ET AL: "SELF AUTHENTICATING PROXIES" COMPUTER JOURNAL,GB,OXFORD UNIVERSITY PRESS, SURREY, vol. 37, no. 5, page 422-428 XP000485456 ISSN: 0010-4620 * page 422, left-hand column, line 1 - page 426, right-hand column, line 6 *	1,7-11	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04L
G06F
H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	5 January 2000	Lievens, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 40 1613

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-01-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5412717 A	02-05-1995	AT 177857 T	15-04-1999
		AU 3820993 A	18-11-1993
		CA 2095087 A	16-11-1993
		DE 69323926 D	22-04-1999
		DE 69323926 T	30-09-1999
		EP 0570123 A	18-11-1993
		ES 2128393 T	16-05-1999
		JP 6103058 A	15-04-1994
		US 5311591 A	10-05-1994
WO 9602993 A	01-02-1996	AU 698454 B	29-10-1998
		AU 3715695 A	16-02-1996
		CA 2194475 A	01-02-1996
		CZ 9700115 A	17-09-1997
		EP 0771499 A	07-05-1997
		JP 10504150 T	14-04-1998
		NO 970084 A	10-03-1997
		TR 970079 A	21-02-1997
		US 5659616 A	19-08-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82